System of secured chip card usable as a digital purse

This invention deals with chip card systems including digital payment systems allowing products purchases by the owner thanks to a chip card without any paper or coin money transfer and deals more specifically with a secured chip card system usable as a digital purse.

The bankcard system already allows this type of transaction, but it is limited to rather high amounts, and it requires a direct link with a bank account.

Several systems of digital purses (DP) have been devised, that allow the presetting of a given amount of money and the purchase of products or services for an amount lower or equal than the available amount of money.

Generally speaking, digital purses are based on standard chip cards. They can be loaded again. In the disposable DP, the electronic module is composed of a standard memory that shows the available amount, which is decremented during each transaction of the relevant amount, until balance reaches zero. This type of digital purse operates exactly like a prepaid phone card. The reload able DP exhibits a more complex structure since it includes a read and write memory including a balance file, which is decremented for each transaction like the disposable DP, or on the contrary incremented with the reloaded amount; all these operations being under the microprocessor monitoring with a security level unattained with disposable cards.

The disposable DP management system requires an acquisition and reloading system and a system allowing the monitoring of transfers of digital money and hence a new architecture compared to the already existing credit card system. For instance, the DP management system requires a system controlling both the remote transmission and the acquisition of digital money. All these DP systems are

reloaded through terminals and offer a lower security level compared to a money chip.

Among the presently known DP systems, the system described in the European patent claim EP 90400280.5 is a flexible process in which the chip card at the disposal of the user includes a permanent chip and a removable chip containing the authorized credit in memory, this credit being decremented during each transaction, the card being housed in a dedicated terminal.

However, since the content of the memory can be modified (it actually is modified during each transaction), it exhibits a more fragile security capability due to the multiple accesses to the memory than a read once chip.

In addition, a system that uses a removable chip not controlled by the Central Money Office may induce a risk of uncontrolled variation of the monetary mass through creation of digital money.

For all these reasons, the aim of this invention is to propose a chip card system, that can be used as digital purse with a permanent module and a removable module, in which it is impossible to modify the credit amount contained in the removable module which is in addition under the central bank control.

The invention deals therefore with a secured chip card system including mainly a card with a first module composed of a microprocessor and a secured programmable memory, and a second disposable module including mainly a read once memory with a preset credit amount at the user disposal, the read once memory having external points of contacts in order to connect with the corresponding contact points of the hand held terminal in which the card has been inserted. The terminal shows communication means in order to communicate with a remote terminal and record a transaction, and connection means to connect the first and second module together in order to

decrement the secured programmable memory of the transaction amount. The read once memory of the second module contains, in addition to the preset credit amount, a unique serial number allocated by the Central Bank like a banknote, the credit amount and the unique number being recorded in the secured programmable memory through the communication means when the card is inserted for the first time in the terminal.

The goals, purposes and characteristics of the invention will appear more clearly when reading the following description referring to the following sketches:

- figure 1 represents a scheme of the two chip card according to the invention equipped with the permanent chip and the removable chip,
- figure 2 represents a scheme of the mechanism for insertion of the removable chip in the two chip card,
- figure 3 represents a scheme of an alternative mechanism of the two chip card according to the invention,
- figure 4 represents a scheme of the hand held terminal in which a two chip card according to the invention has been inserted,
- figure 5 is a block diagram of the system for payment of a transaction with a hand held terminal of figure 4 in which a two chip card according to the invention has been inserted, and
- Figure 6 is a diagram showing the phases of a transaction made with the system of two chip card according to the invention.

The chip card according to the invention also called two chips card is represented on figure 1. Card 1 includes a permanent programmable chip 2 and a removable disposable chip that can de replaced and that corresponds to a preset amount (for instance 100 dollars).

In general terms, the removable chip is clipped in a dedicated slot in card 1. According to the construction

process represented on figure 2, a slot allows the introduction of the card through sliding on male guiding devices 20 on the chip and female guiding devices 20′ on the chip card 1.The external width of the slot B is slightly lower to the internal slot A, allowing card 1 to tightly maintain the removable chip through elastic pressure.

In a construction process represented on figure 3 which allows the reading through contact points of this two chip card by any card reader already fitted, the removable chip 3 is positioned according a full central symmetry compared with permanent chip 2 in order to allow the reading of one chip and then the reading of the other chip, through insertion, withdrawal, rotation, and re-insertion of the chip card 1 in the said reading device which hence can be substituted to the hand held terminal according to the invention in order to allow communication between chips 2 and 3.

Referring to figure 4, the two chip card can be inserted in the handheld terminal 6 fitted with the screen 9 and with the keyboard 10 which includes the keys "validate" "activate", "authorization request" and "transfer", and also communication means 11 using radiofrequency, infrared or any other mean for communication with remote connection means as described below.

The removable chip mainly includes a read once memory such as EPROM which includes a preset credit amount and a unique serial number. Preferably it can be directly issued by the Central Bank, which keeps its money production monopoly, or as an alternative by a bank that stores a sum of money equivalent to the amount of the issued chips being used, under the control of the central bank. This chip is somehow an actual digital bank note with, in addition, the advantage of being directly divisible, while keeping track of these divisions. It can be easily delivered through banks, post offices, and in any authorized location. It has to be noted that, on each removable chip is engraved or clearly stamped part or all of

the chip serial number, this registration being also being shown as a barcode.

The permanent chip 2 is fixed on the card preferably according to ISO standards. This chip mainly includes a microprocessor and a set of highly secured programmable memories (ROM, PROM, and EEPROM) in order to store an identification code for the owner, several parameters such as the profile, category data useful for the user (coupons, reduce rates, access authorizations...). The memories store the transaction management software and a set of algorithms useful in order to allow the best security level. The said memories also store other algorithms that allow others functions described later on. The EEPROM is divided in sections, each section being dedicated to a specific use. The accesses to each section are protected through confidential codes and/or with encryption keys, for instance the access to and the management of memory (5) during every transaction. The possibility of using several sections allows several suppliers such as department stores, airlines to enroll in the system and to load specific applications and to have a focused "marketing" strategy or "data mining".

When the card 1 fitted with a new removable chip is inserted in the handheld terminal 6 for the first time, interconnection means housed in the hand held terminal allow connection between the permanent chip and the removable chip. The microprocessor of the permanent chip then triggers the transfer of the preset amount and of the unique serial number loaded in the read once memory in the removable chip towards the secured memory of the permanent chip through interconnection means (not shown) fitted in the hand held terminal (6).

Once the amount of money set in the removable chip has been transferred in the secured memory of the permanent chip, the removable chip has no value any more and cannot be used

again by the owner. However, the microprocessor will check in sequence and before each transaction that the removable chip is still present in the two chip card for security reasons.

The electronics of the hand held terminal 6 allows first to make chip 2 and 3 of the two chip card to communicate together as described previously, but also to manage data exchange between the communication means (11) and external connection means (12). In every case, the microprocessor of the permanent chip controls data exchange operations through the hand held terminal 6 between the two chip card and the external connection means.

The other functions of the hand held terminal are to provide the power supply of the two chip card which is fitted with batteries, and to allow the reading of chips 2 and 3, including for control, information or security purposes.

The data exchange between the hand held terminal and a variety of connection means 12 is now described, with reference to figure 5. In the most general case, the used connection mean will be a terminal 12'. It is fitted of contact less communication means allowing dialog with the communication means of the hand held terminal 6. It is also fitted with chip card reading device 16 also allowing exchanges with contacts. The terminal 12' is located at the retailer store, service supplier premises, on buses, in parking lots,..., and received a series of payments and other data. The exchanged data between the hand held terminal (6) and terminal (12') are of four types :

(a) data for exchange control: mutual recognition, anti jamming when several hand held terminals transmit together, encryption, etc... These data are used with the only purpose to make reliable exchanges between the hand held terminals 6 and the terminals 12',

(b) data representing the amount of each transaction, the said amounts being stored in a secured memory in the terminal 12',

(d) data allowing the flow management and security: monitoring of the flows of sums of money and security data against fraud, commercial and miscellaneous data: promotion campaign that can be linked with specific data of the owner stored in a memory of the permanent chip, incentive or frequent customer programs, for instance a percentage of some expenses, purchase or service, can be stored in a dedicated memory space in the permanent chip and can be made available by the user under specific conditions.

Regularly, for instance every night, the terminal 12' is connected to a central computerized system 14 to transfer the data (b), (c) and possibly (d) defined above, the said data, stores in a suitable mass storage memory, will allow the calculation of the payment amount of the day and all the data for security and control. The computer system then follows a procedure for processing the data (b) in order to bring to the credit of the account associated with terminal 12' the total amount of payments of the day, and to achieve all necessary controls, checking and useful statistics while processing data (c).

The chip card reading device 16 of the terminal 12' allows, in case of failure of the handheld terminal or of used batteries, to maintain the exchanges through contact by sliding the chip card 1 in the reading device 16. According to another production mean of the terminal 12', the later can be portable, like the existing digital payment terminals.

A second type of connection means 12'' consists in specific terminals installed in dedicated location, for instance in banks. These terminals are different from the previous ones since they are permanently connected to the central computer system 14. The specific terminals 12'' allow

the user to make several bank transactions. These transactions have been previously typed in through the keyboard 10 of the hand held terminal 6 and recorded in the memory of the permanent chip 2. The microprocessor of the permanent chip asks the user to type in a preset confidential code or Pin Number before recording the requests defining the transactions in a memory of the chip 2. The user may then transmit the prerecorded transactions (or information requests) thanks to the contact less link authorized by the hand held terminal 6 or by insertion of the card 1 in the reading device 16' of the terminal 12''. The terminal 12'' can also transmit towards the hand held terminal 6 every useful data that will be stored in the memory of the permanent chip 2.

A third type of external communication mean consist in a personal computer 12'''connected to the Internet network, to a switched network, or other. The permanent chip 2 of the chip card stores in its EPROM memory software files and one or several algorithms that can deliver an authorization number associated with a well defined transaction. Those pieces of software and algorithms are also stored on the sales site 21 of the supplier of goods or remote services operating on the Internet network. The following example will help to better understand:

Mister Phil Jones wants to buy some good on an Internet sales site. He makes the connection to the selected site that proposes to him a list of products with their associated prices. Mister Phil Jones selects the article or articles of his choice. The sales site 21 then displays the list of selected items and the price to be paid. If M. Phil Jones agrees with this list, he confirms his order. The sales site will ask for his contact points (name, surname, address) and the selected mode of payment.

Mister Phil Jones holding the hand held terminal 6 in which his own two chip card according to the invention is

inserted then needs to type in through the keyboard of the hand held terminal the parameter of the on going purchase and specifically the amount to be paid and to press the key: "authorization request".

The algorithm stored in the EPROM memory of the permanent chip will consider some or all the following parameters: name, surname, address, date, amount to be paid, number of the processed money chip. If the microprocessor assess that the transaction is possible (enough credit, minimum age limit, …), it assesses through the algorithm an authorization number specific for each on going transaction. The serial number of the removable chip and the authorization number that has been computed are then displayed on screen 9 of the hand held terminal. Once these elements are displayed, the amount of the transaction is immediately debited in the secured memory of the permanent chip.

Mister Jones then communicates to the sales site through the keyboard of his computer 12''' the data displayed on the screen. The computer of the sales site 21 having the same algorithms, assesses now an authorization number and validates the coherence with the number that the purchaser has just sent, and then validates or rejects the order, and the money transaction recorded or rejected.

A similar procedure may be used from a phone set 12''''. In this configuration, the buyer can communicate with a robot through recognition and synthesis of speech or through a human operator. The validation of the transaction is then made by introduction on the phone set keyboard using the voice frequencies (DTMF), of the elements defined above (removable chip serial number and authorization number displayed on the screen 9 of the hand held terminal 6.

During the first payment operation using the credit of a new removable chip 3, the chip serial number is automatically

transmitted to the terminal 12 with a code "new chip n° x activated), in addition to the amount of the transaction. This information is then transmitted again towards the central computer system 14 which manages the chip monitoring during the remote collecting of the retailer terminals.

In a similar fashion, each time the secured memory of the permanent chip is totally using up the credit amount received from a removable chip during the payment transaction, the serial number of the removable chip being fully used up is transmitted to the terminal 12 with a code "chip n° y used up" in addition of the transaction amount, this information is transferred to the central computer system 14 as mentioned previously.

This way the management body may accurately know, in real time:

1/ all the issued removable chips and distributed and non initialized (eventually piled up),

2/ all the issued removable chips being used,

3/ all the fully used up removable chips.

All these three key pieces of information allow the accurate monitoring of the issued digital money volumes, being used, piles up or used up. Any attempt of emission of forged digital money is then immediately assessed. Hence, this system represents a very strong forgery deterrent. Hence, a load of stolen chips can be immediately opposed to through transmission to the terminals (12, 12',...) of a black list of stolen chip serial numbers.

Therefore this system also allows the Central Bank to accurately know the state of monetary mass and / or the issuing Bank to better manage the sums of money to be deposited versus the issued chips.

A variation of the procedure described above consists in systematically communicating, during each transaction, the

serial number of the removable chip, which allows a more accurate monitoring, but with a higher data to manage.

The transactions:

Each transaction between the hand held terminal and the terminal at the sales store is going through three phases:

1. The sales person types in the price on his keyboard. This price is simultaneously transferred to the user hand held terminal.
2. The customer sends his agreement by pressing the key "validation" of his hand held terminal.
3. The secured memory of the permanent chip 2 that has previously been loaded with a removable chip 3 is then debited with the amount of the transaction and the memory of the sales store terminal is credited with the same amount.

As explained above, the chip card 1 can process transactions without hand held terminal and through contact. In this case, the positioning of the permanent chip is according to the ISO standards, which allows a large majority of present reading devices to process transactions without modification of the equipment, by using an application software that can be downloaded during a connection with the central computer system 14.

In case of a contact less reading,

The various steps of the transaction are described on the flow chart, represented on figure 6:

1/ Activation of the hand held terminal by pressing the key "activate" of the hand held terminal 6.

2/ Control of the presence of the removable chip by the microprocessor of the permanent chip, and checking that the serial number of this chip matches the number that has allowed the re-loading of the memory. If the control is not positive, an error message is displayed on screen 9 and the electronics is activated.

3/ If the control is positive, the microprocessor stores the control parameters including the time, date of the said control and gives a temporary authorization for transaction.

If the payment is made contact less :

5/ The sales person dials the price to be paid on the keyboard of the terminal 12.

6/ The terminal transmits and exchanges data a) with the microprocessor in order to achieve mutual recognition.

7/ The transaction amount is transmitted from terminal 12 to the hand held terminal 6.

8/ The said amount is displayed on the screen of the hand held terminal 6.

9/ If the owner does press the key "validate", the transaction is cancelled. If, like in most cases, the owner presses the key "validate", then,

10/ The microprocessor performs the analysis of the feasibility of the operation :

- Enough credit or acceptable temporary credit,
- Temporary authorization of the valid transaction (stage 3),
- Analysis of the profile parameters stored in the permanent memory and possible modifications of the transaction amount or cancellation (rebate, minimum age limit…).

11/ If phase 10 is satisfactory, the hand held terminal and the terminal exchange the data b) c) d). If phase 10 is not satisfactory, the transaction is cancelled.

12/ The transaction is made:

- Debit of the removable chip of the buyer,
- Credit with the same amount of the memory of the retailer terminal,
- Storage of data c) and d) in the retailer terminal,
- Storage as required of the data d) in the memory of the permanent chip of the chip card.

If the payment is made with contact:

5'/ The retailer types the price to be paid on the keyboard of the terminal 12,

6'/ The customer owning the chip card inserts it in the card reading device of the terminal 12,

7'/ The microprocessor analyses the validity of the temporary authorization (stage 3). If the validation is satisfactory, then phase 10 is followed, otherwise the transaction is cancelled.

Five categories of bodies are involved in the transaction as per the invention:

- The issuer of cards provides the population with:

Hand held terminals

Cards only fitted with one permanent chip

- The issuer of removable chips: the central bank or any authorized bank,
- The user, owner of the hand held terminal,
- The transaction maker: retailers or suppliers equipped with connection means (12', 12'', 12''', 12'''')
- The collector: one or several bank facilities or local financial bodies, tasked to credit the retailers accounts daily.

Depending on the specific construction mode, two hand held terminals, one sending and one receiving, fitted with their chip card, may also exchange small amounts of money. In order to achieve the data exchanges allowing the money transfer from one to the other, both terminals must be close and must face each other if the infrared is used as the communication mean. Such transaction must meet the security criteria, anonymity needs and the responsibility requirements of the receiver in order to avoid fraud.

Assuming that the first hand held terminal has to transfer a sum of 3 $ to the other one, the owner of the sending hand held terminal types the transfer amount on the keyboard of the

said hand held terminal, and presses the transfer key. The owner of the receiving hand held terminal located at a short distance, must then press the "activate" key.

- The first hand held terminal takes 3 $ off the secured memory of the permanent chip located in the hand held terminal, and transmits this amount along with the serial number of the removable chip that has allowed to credit the secured memory to the receiving hand held terminal which is expecting the information.
- The 3$ amount is displayed on the screen of the receiving hand held terminal and then is credited in a secured memory of the permanent chip of the chip card located in the receiving terminal, this specific memory being allocated to the received amounts from another hand held terminal according to the procedure just described. In addition, the serial number of the removable chip located in the transmitting hand held terminal is also stored in this memory, this serial number being associated with the transaction that has just occurred.

For security reasons, this procedure can be used only a small number of times (3 to 5 for instance) and can only be applied to small amounts. For the first payments that will be made by the owner of the chip card inserted in the hand held terminal that has received a sum of money from another chip card via the exchanges between two handheld terminals, it is the amount(s) stored in the permanent chip that will be spend first.

The permanent memory that allows the storage sums of money sent by another chip card via a hand held terminal, can record several transactions as described above. The permanent memory records the parameters relevant to each transaction (serial number of the removable chip of the sender and the received amount, and in order to make the receiver responsible, his identification code), these parameters being transmitted to

the computer system 14 for every payment operation, as long as the recorded amount in the permanent memory is not used up.

Many variations of the invention may be considered. For instance, the removable chip may be representative of a loan, the permanent chip then recording the management data of the loan, generating automatically the reimbursement payments, transmitted during a connection with a connection mean 12.

It has to be noted that, according to a variation, if the available credit stored in the permanent memory is not sufficient to make the payment, it can be considered that the microprocessor will still make the payment in the limit of the authorized temporary credit which preset amount is stored in the permanent memory, this temporary credit being reimbursed as soon as a new removable chip is inserted.

Finally, on can easily imagine that the chip card includes, in addition to the slot for installation of removable chip, a second or even a third slot in order to introduce other chips containing for instance specific money values, coupons, games, parameters for accessing secured locations,... In this assumption, the hand held terminal must be fitted with the relevant connectors.

The system described previously is a digital purse with a universal target, that can involve hundred per cent of a population, with or without bank account, without any obligation to own a bank card for reloading, It can process all the operations and has the same advantages as the conventional money (anonymous payments, possible piling up) while providing to the bank institutions such significant advantages like centralized and secured issuing of money, and the automated monitoring of flows.

Another application of the concepts of the invention tackles forgery. A certification chip is attached to all luxury or expensive items (watches, jewelry...) with any known

mean, the certification chip being removed from the item by the seller during the sale.

The certification chip actually is a removable chip that, during a crosscheck, must be inserted in the slot of the chip card 2. Like previously, the chip is operated via a hand held terminal 6, thanks to at least one algorithm stored in the permanent memory. It includes two memory zones. The first zone stores an identification code and a unique serial number of the item. For instance: "luggage: model x, color y, serial n° z". The seller of the luxury item is equipped with a terminal fitted with means that allow the writing, only once and during the sale, in the second memory zone the parameters of the sale (date, seller name, amount, warranty and associated conditions, possibly the name of the future owner)…

The certification of the sold item is made through the insertion of the chip card fitted with the certification in the hand held terminal. The microprocessor of the permanent chip, through at least one algorithm stored in the EPROM memory, is able to read the pieces of information contained in the memories of the chip and to check its coherence.